REMARKS

The Examiner is thanked for the careful review of this application.

Favorable reconsideration and allowance of the present patent application are respectfully requested in view of the foregoing amendments and the following remarks. Claims 1-24 are pending in the current application. Claims 1, 10, 11, 18, and 19 are independent claims.

Rejection under 35 U.S.C. §101

Claims 19-21 are rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. By the present Amendment, the language of "non-transitory" has been added to the preamble of independent claim 19, such that claims 19-21 no longer read upon non-transitory media. In view of the amendment to independent claim 19, the Applicants respectfully request that the Office withdraw this rejection.

Rejection under 35 U.S.C. §103(a) over Koskimies in view of Brody

Claims 1-7, 9-14, 16-24 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication No. 2004/0081110 ("Koskimies") in view of U.S. Publication No. 2001/0051928 ("Brody"). The Applicants respectfully traverse this art ground of rejection.

Koskimies is directed to a system and method for downloading data to a limited device, whereby a target device requests content from a data storage system, and the data storage system responds with the requested content (e.g., [0011], Koskimies). In Koskimies, the request for content from the target device is described as an "SMS content request," and the download of the requested content is conveyed via "an SMS message with the download information" (e.g., [0065] of Koskimies). Paragraphs [0077]-[0083] of Koskimies describe Digital Rights Management (DRM) that is used to secure the content against unauthorized copying. As

described at [0079]-[0080], a secret code is generated for the target device and is made available to the target device and the trusted download server (or data storage system) that is providing the content. Then, the requested content from the trusted download server is encrypted and can only be decrypted by the target device via the use of the secret code (e.g., [0079]-[0081] of Koskimies). Therefore, Koskimies states that "[s]ince content will only work with a single target device, copying the content is of no use" (e.g., [0083] of Koskimies).

Accordingly, the security protocol discussed by Koskimies is DRM that is based on encryption of content via some type of secret code. Accordingly, in the context of Koskimies' disclosure, downloading an application in compliance with the security protocol means the content is encrypted via the secret code, and downloading the application without compliance with the security protocol means the content is not encrypted via the secret code.

Firstly, it will be appreciated that the requested content is conveyed to the target device from the content server via an SMS or text message (e.g., see [0065] of Koskimies). It is unlikely that the content's status as being encrypted or unencrypted would affect the manner in which the target device downloads the SMS message carrying the requested content. Rather, the SMS message carrying the requested, encrypted content is likely conveyed to the target device in the same manner as an SMS message with unencrypted content. The issue of whether the target device is capable of decrypting the content only factors into whether the target device can access the content *after* the download. In other words, the DRM security protocol is based on evaluating the downloaded content and controlling the manner in which the downloaded content can be accessed by the target device, **not** the manner in which the content is downloaded to the target device in the first place. Thus, Koskimies does not appear to disclose or suggest both "a resident application environment configured to selectively download applications … that comply with a predefined security protocol" and "a download manager … that is configured to

selectively download applications … that do not comply with the predefined security protocol" as recited in independent claim 1 and similarly recited in independent claims 10, 11, 18 and 19.

Secondly, a stated objective in Koskimies is to ensure that only the target device can decode its own requested content. In Koskimies, to permit downloading of content without the DRM security protocol corresponds to permitting the content to be exposed to unauthorized users. Accordingly, Koskimies clearly suggests using DRM to secure its content downloads, and does not disclose or suggest "a download manager … that is configured to selectively download applications … that do not comply with the predefined security protocol" as recited in independent claim 1 and similarly recited in independent claims 10, 11, 18 and 19.

The Applicants note that the Office appears to make an admission regarding the above-noted deficiencies of Koskimies. However, the language used by the Office renders this admission unclear. For example, the Office states:

> Koskimies states a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol but Brody particularly points out a download manager resident on the computer platform that at least selectively downloads applications that do not comply with the predefined security protocol (Paragraph 22). *(e.g., see Page 5 of the Office Action)*

Thus, the Office appears to indicate that Koskimies does actually disclose the download manager, such that it is unclear why the Office cites to Brody. In any case, the Applicants have shown above that Koskimies does not actually disclose the "download manager" as claimed. Further, the Applicants have reviewed Brody and likewise submit that Brody also fails to disclose or suggest the "download manager" as claimed.

Brody is directed to protection of software by personalization, whereby unauthorized copying of the software is discouraged by "personalizing" the software to each authorized user of the software (e.g., Brody, Abstract). The Office primarily cites to [0022] of Brody for

allegedly disclosing "a download manager … that is configured to selectively download applications … that do not comply with the predefined security protocol" as recited in independent claim 1 and similarly recited in independent claims 10, 11, 18 and 19. In Brody at [0022], Brody describes applying a digital signature to Java applets such that if the digital signature is recognized by the target device "the corresponding Java software application is given access to more extensive resources of the user's computer" and "can be executed in a normal fashion" (e.g., [0022] of Brody).

As will be appreciated, similar to Koskimies, the Java applet must be downloaded before the digital signature (or personalized encryption) can be evaluated and/or authenticated. In other words, security protocol in Brody relies upon the target device evaluating the digital signature and then controlling the manner in which the Java applet is executed, **not** the manner in which the Java applet is downloaded in the first place. The Applicants believes this teaches away from configuring the target device to include both "a resident application environment configured to selectively download applications … that comply with a predefined security protocol" and "a download manager … that is configured to selectively download applications … that do not comply with the predefined security protocol" as recited in independent claim 1 and similarly recited in independent claims 10, 11, 18 and 19.

Also, similar to Koskimies, a stated objective in Brody is to ensure that only the target device can decrypt and/or execute its authorized Java applets. In Brody, to permit downloading of the Java applet without the security protocol (i.e., the digital signature and/or personalization) corresponds to sending the Java applets without encryption, which exposes the application to unauthorized users. Accordingly, similar to Koskimies, Brody does not disclose or suggest "a download manager … that is configured to selectively download applications … that do not

comply with the predefined security protocol" as recited in independent claim 1 and similarly recited in independent claims 10, 11, 18 and 19.

In view of the deficiencies shared by both Koskimies and Brody as discussed above, the Applicants respectfully submit that independent claims 1, 10, 11, 18 and 19 are each allowable over the combination of Koskimies in view of Brody. As such, claims 2-7, 9, 11-14, 16-17 and 20-24, dependent upon independent claims 1, 11, 18 and 19, respectively, are likewise allowable over Koskimies in view of Brody at least by virtue of their dependence upon the independent claims.

The Applicants respectfully request that the Office withdraw this art grounds of rejection.

Rejection under 35 U.S.C. §103(a) over Koskimies in view of Brody in view of Hericourt

Claims 8 and 15 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Publication No. 2004/0081110 ("Koskimies") in view of U.S. Publication No. 2001/0051928 ("Brody") in further view of U.S. Patent No. 7,099,916 ("Hericourt"). The Applicants respectfully traverse this art ground of rejection.

As an initial matter, the Applicants agree with the Office's admission that Koskimies and Brody fail to disclose features specific to dependent claims 8 and 15 (e.g., see Pages 14-15 of the Office Action). The Office alleges that Hericourt cures these particular deficiencies of Koskimies and Brody. Hericourt is directed to a system and method for downloading a virus-free file certificate from a file server, whereby the file certificate is provided to a requesting entity to verify that a certificate is virus-free (e.g., Hericourt, Abstract). Even assuming for the sake of argument that Hericourt discloses the features specific to claims 8 and 15 (which the Applicants do not admit), the Applicants respectfully submit that a review of Hericourt indicates

that Hericourt is insufficient to cure the suggestion and disclosure deficiencies of Koskimies and/or Brody as discussed above with respect to independent claims 1 and 11.

As such, claims 8 and 15, dependent upon independent claims 1 and 11, respectively, are likewise allowable over Koskimies in view of Brody in view of Hericourt at least by virtue of their dependence upon the independent claims.

The Applicants respectfully request that the Office withdraw this art grounds of rejection

CONCLUSION

In light of the amendments contained herein, Applicants submit that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated October 5, 2010

By: /Fariba Yadegar-Bandari/
Fariba Yadegar-Bandari
Reg. No. 53,805
(858) 651-0397

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502